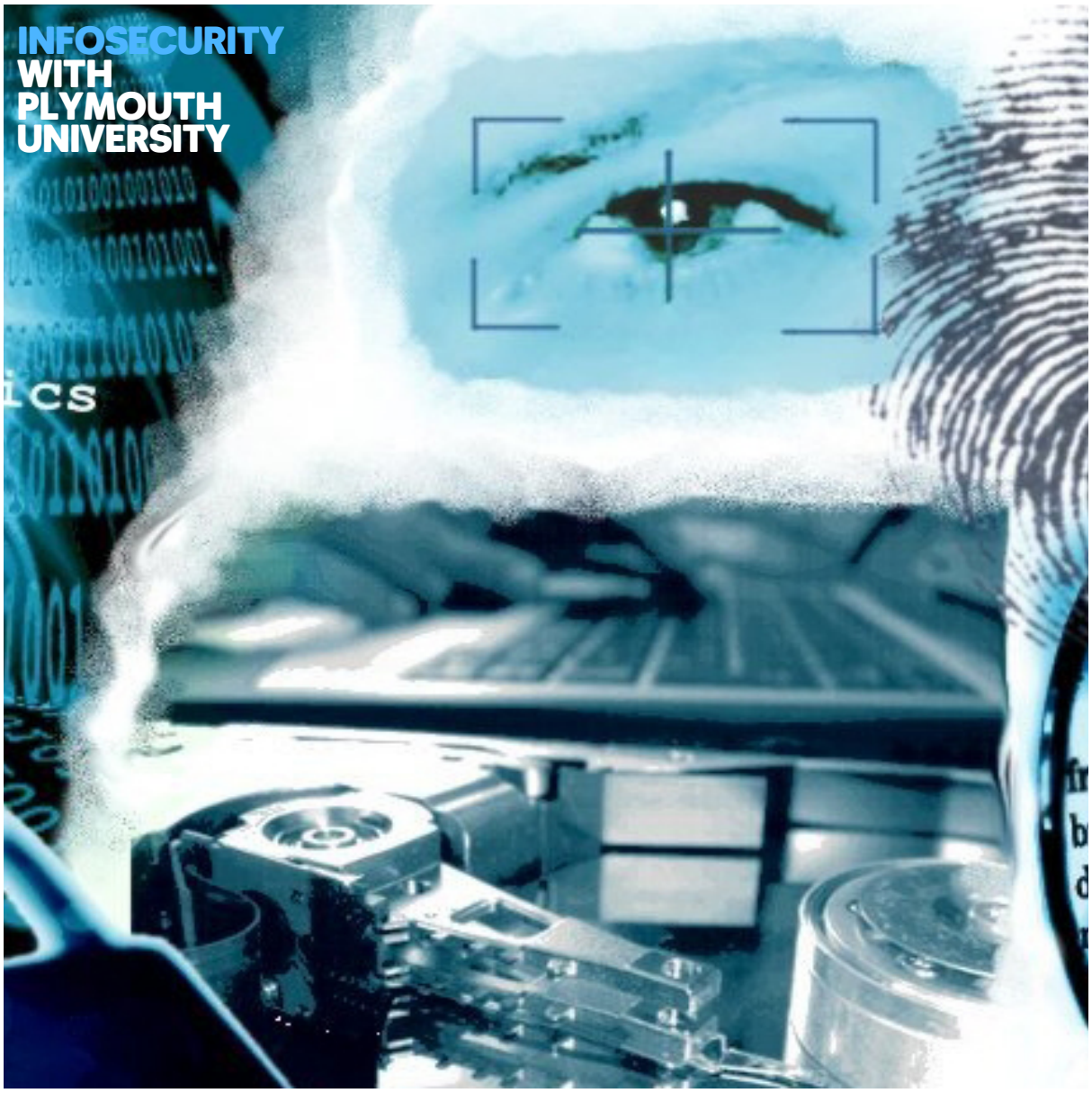
THE ESSENTIAL GUIDE TO ...



PROTECTING YOURSELF ONLINE

TEN TOP TIPS FOR INTERNET SECURITY

1. **Install and run Internet Security software**

   This will provide protection against viruses and attacks and block intruders from accessing your computer. See the list of examples on the next page.

2. **Ensure that your Internet Security / antivirus protection is up-to-date**

   Thousands of new viruses and other attacks appear every day and if your system doesn't know about them, or your subscription has expired, then you will not be protected against the most likely problems.

3. **Enable automatic software updates for your computer**

   Companies often release security-related updates, and if you do not install them you are giving hackers and viruses an opportunity to attack your computer.

4. **Make sure that encryption is enabled on your wireless network**

   This will prevent attackers from using your network or spying on your data. Look for WPA protection in preference to (older and weaker) WEP options.

5. **Beware of fake security warnings and other online scams**

   Fake security emails and pop-up windows can claim that your system has been attacked and try to trick you into downloading something that will actually attack you! Meanwhile, other messages are designed to trick you into giving away sensitive information. Running genuine Internet Security tools will help to block these.

6. **Use secure passwords**

   These are still the most common way to verify your identity online, and so you need to use them properly to prevent someone pretending to be you.

7. **Take backups of your data**

   This will ensure that you do not lose anything if your system is attacked or if your computer fails.

8. **Be careful when entering personal data online**

   Things like your address, date of birth and (especially) financial details are very interesting to attackers. If you give away enough personal information, someone could use it to attack you or access your accounts.

9. **If you're making online payments, expect extra security**

   Look for sites that support Verified by Visa and MasterCard SecureCode (you need to register with these schemes first, but you can then be more sure that you're using genuine sites).

10. **Read a bit more about the topic to ensure that you're fully informed**

    As a good source for further details visit www.getsafeonline.org

HOW TO CHOOSE GOOD PASSWORDS

✓ **Do use at least 8 characters and mixture of character types (letters, numbers, symbols)**

This makes it harder for an automated password-cracking program to try all of the possible combinations.

✓ **Do change your password regularly**

If someone has discovered it without your knowledge, this will stop them getting any further access.

✓ **Do use different passwords on different systems**

If your password is discovered on one system, the others won't be at risk.

X **Don't give your password to someone else**

Your password is meant to be a secret. If someone else knows it then they can pretend to be you.

X **Don't use a word that you would find in the dictionary or any personal details about yourself**

Because these can be more easily guessed by cracking programs or people that know you.

X **Don't write your password down somewhere that it could be found**

Because someone could find it!

X **Don't allow the computer to remember your password on a shared or public system.**

An impostor would only need to know your username in order to get access, as the system would automatically provide the password for them.

☑ A good way to remember a complex-looking password is to remember the first letters of a phrase:

10GBsotw.	**10** **G**reen **B**ottles **s**tanding **o**n **t**he **w**all**.**
CdViaci101D!	**C**ruella **d**e **V**il **i**s **a** **c**haracter **i**n **101** **D**almatians**!**

☑ Another way is to use something that is meaningless, but still pronounceable (e.g. **ClemPoggle34!!**). Being able to say the word can help you to remember it more easily. And yet another method is to substitute letters for numbers. For example: **5tr0ngP@55w0rd!.**

☑ The more information you are storing on a system or site, the better the password you should use.

☑ Use a password strength meter to ensure your password is strong enough. Some sites have these built in, but you can also try **www.passwordmeter.com** or our own one at **www.cscan.org/passwordstrength**.

☑ Don't worry about remembering passwords for sites that you don't intend to use very often (you could just use the 'forgotten password' link when you want to log in).

☑ Remember to sign out of websites once you have finished your session, otherwise the next user won't need a password because you're still logged in.

INFOSECURITY WITH PLYMOUTH UNIVERSITY

SOME FREE SOURCES OF INTERNET SECURITY PROTECTION

If you are not already running an Internet Security or antivirus package, then the links below can help to check whether your system is safe.

Please note that we are not specifically endorsing any of the products or services, but are providing the links so that you are led to some genuine sites from which you can make a choice. Doing a search for 'free antivirus' (or similar) is **not** a safe option, as some results may point to malicious sites masquerading as protection tools.

FREE ANTIVIRUS TOOLS	
avast! Free Antivirus	www.avast.com/free-antivirus-download
AVG Free Antivirus	free.avg.com
Avira AntiVir Personal	www.avira.com/free
LEADING COMMERCIAL VENDORS THAT OFFER FREE TRIAL VERSIONS, REMOVAL TOOLS AND/OR ONLINE SYSTEM SCANS	
Kaspersky Lab	www.kaspersky.com/virusscanner
McAfee	home.mcafee.com/downloads/free-virus-scan
Norton	security.symantec.com/sscv6
Sophos	www.sophos.com/en-us/products/free-tools.aspx
Trend Micro	housecall.trendmicro.com/uk/

Visit our research centre website

www.plymouth.ac.uk/cscan

Get our free security podcasts on iTunes

www.cscan.org/podcasts

Centre for Security, Communications and Network Research
Plymouth University, Plymouth, PL4 8AA
cscan@plymouth.ac.uk
www.plymouth.ac.uk/cscan